ZENTRALER IT-BETRIEB
NIEDERSÄCHSISCHE JUSTIZ

# Informationen zur sicheren E-Mail-Kommunikation mit der Nds. Justiz

| | |
|---|---|
| Ersteller: | Carsten Tesch |
| am: | 25.03.2019 |
| Version: | 1.0 |
| Status: | Endgültig |

ZENTRALER IT-BETRIEB
NIEDERSÄCHSISCHE JUSTIZ

## Inhaltsverzeichnis

## 1. Vorwort

E-Mail ist heute für Unternehmen ein häufig eingesetztes Kommunikationsmittel, das zum Austausch von Informationen verwendet wird. Auch die Nds. Justiz steht mit einer Vielzahl von Kommunikationspartnern per E-Mail in Kontakt.

Die Informationen, die über E-Mail ausgetauscht werden, sind dabei meist auch vertraulich, so dass sie besonders vor Manipulation und fremdem Zugriff geschützt werden müssen. Ohne eine gesonderte Absicherung ist die Datenübermittlung im Internet zwischen Absender und Empfänger völlig ungeschützt und vergleichbar mit dem Versand einer mit Bleistift beschriebenen Postkarte. Für einen wirkungsvollen Schutz der E-Mail-Kommunikation sind deshalb zusätzliche Sicherheitsmaßnahmen zwingend erforderlich.

Um vertrauliche Informationen in E-Mails zu schützen, verwendet die Nds. Justiz sichere Standardverfahren zum Austausch von verschlüsselten E-Mails.

Der sichere E-Mail Kommunikationsweg mit S/MIME und PGP steht ausschließlich für Verwaltungsangelegenheiten zur Verfügung. Es wird darauf hingewiesen, dass mit diesem Kommunikationsmittel Verfahrensanträge oder Schriftsätze nicht rechtswirksam eingereicht werden können. Für die rechtswirksame Kommunikation nutzen Sie bitte das elektronische Gerichts- und Verwaltungspostfach (EGVP) bzw. DE-Mail. Beachten Sie dazu bitte die Hinweise auf den Internetseiten der jeweiligen Justizbehörden. Dort finden Sie auch die jeweiligen Kontakt-Adressen der einzelnen Behörden!

Die Nds. Justiz möchte Ihnen mit diesem Dokument alle Informationen bereitstellen, die notwendig sind, um einen sicheren Kommunikationsweg zwischen Ihnen und der Nds. Justiz aufbauen zu können Im Folgenden werden die relevanten Begriffe im Zusammenhang mit E-Mail-Verschlüsselung und die grundlegenden Schritte zur Konfiguration und Einrichtung eines sicheren

Kommunikationssystems erläutert. Am Ende dieses Dokuments finden Sie hierzu eine kurze Anleitung.

Bei Fragen bezüglich E-Mail-Verschlüsselung in Verbindung mit der in Ihrem Unternehmen eingesetzten E-Mail-Lösung wenden Sie sich bitte an die entsprechenden technischen Ansprechpartner in Ihrem Unternehmen.

## 2. Begriffserläuterungen

### Verschlüsselung

Um die Vertraulichkeit einer E-Mail-Kommunikation zu wahren, müssen E-Mails verschlüsselt werden. Die notwendigen Informationen, die zum Ver- und Entschlüsseln von E-Mails benötigt werden, sind in einem sogenannten digitalen Zertifikat enthalten. Bevor ein gesicherter Austausch von Informationen in Form von verschlüsselten E-Mails stattfinden kann, müssen beide Kommunikationspartner über ein digitales Zertifikat verfügen.

### Digitale Zertifikate

Mit einem digitalen Zertifikat kann sichergestellt werden, dass nur der vom Absender adressierte Empfänger einer E-Mail die darin enthaltenen Informationen in einer lesbaren Form erhält. Ein solches Zertifikat, auch Benutzerzertifikat genannt, wird für eine E-Mail-Adresse ausgestellt. Das Zertifikat ist eine digitale Beglaubigung der Identität des Absenders und wird zum einen als eine sogenannte digitale Signatur von E-Mails verwendet, zum anderen können damit E-Mails verschlüsselt werden.

Durch die Beglaubigung kann die zertifizierte E-Mail-Adresse über einen definierten Zeitraum als gültig angesehen werden. Die Gültigkeitsdauer eines digitalen Zertifikats beträgt in der Regel zwischen ein und fünf Jahren.

### Öffentliche und private Schlüssel

Ein Benutzerzertifikat besteht aus zwei Teilen: einem öffentlichen und einem privaten Schlüssel. Der private Schlüssel wird für die Signierung und Entschlüsselung von E-Mails verwendet und darf nie veröffentlicht werden. Der öffentliche Schlüssel muss dem Kommunikationspartner zur Verfügung gestellt werden, damit er die Signatur einer E-Mail überprüfen und verschlüsselte E-Mails an den Besitzer des öffentlichen Schlüssels versenden kann.

Vor der ersten Verschlüsselung von E-Mails muss der Absender den öffentlichen Schlüssel als Teil des Benutzerzertifikats des Empfängers der E-Mail erhalten haben. Dieser Austausch erfolgt in der Regel durch den Versand einer signierten E-Mail. Dieser E-Mail kann der Empfänger dann den öffentlichen Schlüssel entnehmen. Erst dann kann der Absender die E-Mail mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Nach dem Erhalt der verschlüsselten E-Mail kann der Empfänger diese mit seinem privaten Schlüssel entschlüsseln. Diese Vorgänge werden von den meisten E-Mail-Programmen automatisch durchgeführt.

## Signaturen

Damit die Echtheit einer E-Mail-Adresse automatisch überprüft werden kann, wird eine digitale Signatur benötigt. Durch sie kann der Absender einer E-Mail eindeutig identifiziert werden. Außerdem wird mit ihr die Unversehrtheit der E-Mail garantiert, da bei einer nachträglichen Änderung der Daten die digitale Signatur – ähnlich einem gebrochenen Siegel eines Briefes – zerstört wird. Beim Signieren einer E-Mail wird deshalb immer der öffentliche Schlüssel des Zertifikats an die E-Mail angehängt, damit der Empfänger die Echtheit und Unversehrtheit der E-Mail prüfen kann.

Durch die Signierung einer E-Mail können die darin enthaltenen Informationen nicht geändert werden, ohne dass es der Empfänger bemerkt. Sie sind aber weiterhin offen lesbar. Um die Vertraulichkeit beim Informationsaustausch zu gewährleisten, muss die E-Mail zusätzlich verschlüsselt werden. Das sicherste Verfahren zum Austausch von E-Mails ist die Kombination von Signatur und Verschlüsselung.

## S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein weltweit eingesetztes Standardverfahren für den gesicherten Austausch von Informationen per E-Mail mit Zertifikaten. Die notwendigen Komponenten für S/MIME sind in den meisten modernen E-Mail-Programmen bereits integriert, so dass eine einfache und transparente Handhabung gewährleistet ist. Das bedeutet, dass E-Mails durch die Aktivierung der entsprechenden Option im E-Mail-Programm vor dem Versand automatisch verschlüsselt und beim Empfang automatisch entschlüsselt werden.

Die Nds. Justiz akzeptiert neben dem S/MIME-Verfahren auch das Verfahren PGP zur E-Mail-Verschlüsselung.

## PGP

Die sogenannte PGP-Verschlüsselung bietet eine Möglichkeit, Informationen zu schützen und die Inhalte Ihrer E-Mails zu verschlüsseln. Ursprünglich wurde der Begriff PGP – eine Abkürzung für „Pretty Good Privacy“ (dt. „ziemlich gute Privatsphäre“) – für eine bereits 1991 von Phil Zimmermann entwickelte Software zur E-Mail-Verschlüsselung verwendet. Im Laufe der Jahre hat sich der Name jedoch allgemein als Bezeichnung für die von dieser Software genutzte Verschlüsselungsmethodik durchgesetzt.

Die PGP-Verschlüsselung beruht auf einem Public-Key-Verfahren, in dem man ein fest zugeordnetes Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel (Key), verwendet. Der öffentliche Schlüssel wird für potenzielle Mail-Kontakte frei verfügbar gemacht, indem man ihn direkt übermittelt oder auf einem externen Key-Server hoch lädt. Mithilfe dieses Keys verschlüsseln Ihre Kontakte alle elektronischen Nachrichten, die sie Ihnen senden. Der private Schlüssel ist ausschließlich in Ihrem Besitz und für gewöhnlich zusätzlich durch ein Passwort geschützt. Mit seiner Hilfe entschlüsseln Sie erhaltene Mails, die zuvor mit dem öffentlichen Key codiert

wurden. Damit Sie auf diese Weise gesichert kommunizieren können, muss auch Ihr Kommunikationspartner PGP nutzen und Ihnen seinen öffentlichen Schlüssel mitteilen. Das Public-Key-Verfahren wird auch als asymmetrisches Verfahren bezeichnet, da beide Parteien unterschiedliche Schlüssel verwenden. Mithilfe von Signaturen garantieren Sie zusätzlich die Authentizität Ihrer Nachrichten.

**Zertifikatsdiensteanbieter**

Ein Zertifikatsdiensteanbieter (auch Trust-Center genannt) ist eine Organisation, die digitale Benutzerzertifikate herausgibt und für deren Bereitstellung, Zuweisung und Integritätssicherung verantwortlich ist. Sofern Sie über ein S/MIME-fähiges E-Mail-System verfügen, aber noch kein eigenes E-Mail-Zertifikat besitzen, können Sie dieses bei einem Zertifikatsdiensteanbieter beantragen. Der Zertifikatsservice der Anbieter ist in der Regel kostenpflichtig.

**Stammzertifikat**

Zusätzlich zu dem Benutzerzertifikat wird bei der E-Mail-Kommunikation mit der Nds. Justiz auch ein sogenanntes Stammzertifikat benötigt. Mit diesem kann der Vertrauensstatus der Benutzerzertifikate der Nds. Justiz überprüft werden. Das bedeutet, dass das von Ihnen eingesetzte System überprüfen kann, ob das Benutzerzertifikat wirklich von der Nds. Justiz stammt und ob es noch gültig ist.

**Zertifikatsaustausch**

Der Zertifikatsaustausch zwischen den Kommunikationspartnern muss nur einmal vor dem ersten Verschlüsseln durchgeführt werden und ist danach erst wieder notwendig, wenn eines der ausgetauschten Zertifikate seine Gültigkeit verliert.

ZENTRALER IT-BETRIEB
NIEDERSÄCHSISCHE JUSTIZ

## Zertifikat an die Nds. Justiz übermitteln

Wenn Sie Ihr persönliches Benutzerzertifikat von einem Zertifikatsdiensteanbieter erworben haben, brauchen Sie Ihrem Kommunikationspartner in der Nds. Justiz für die Bereitstellung des öffentlichen Schlüssels nur einmalig eine signierte E-Mail zusenden. Diesen Vorgang müssen Sie erst wiederholen, wenn sich Ihr Benutzerzertifikat geändert hat, z.B. aufgrund des Wechsels Ihres Zertifikatsanbieters.

## Zertifikate von der Nds. Justiz erhalten

Das jeweilige Benutzerzertifikat erhalten Sie durch eine signierte E-Mail von Ihrem Kommunikationspartner in der Nds. Justiz. Das Stammzertifikat muss für die Überprüfung der Benutzerzertifikate der Nds. Justiz auf Ihrem Endgerät (z. B. PC) einmalig importiert werden. Das Benutzerzertifikat muss dem entsprechenden Kontakt in dem eingesetzten E-Mail-Programm zugeordnet werden.

Die Gültigkeit der Benutzerzertifikate der Nds. Justiz beträgt drei Jahre.

Das Stammzertifikat der Nds. Justiz kann über die Adresse https://cert.justiz.niedersachsen.de heruntergeladen werden.

## 3. Anleitung S/MIME

1. **Import** des Stammzertifikats der Nds. Justiz
   Das Stammzertifikats der Nds. Justiz kann unter der Adresse https://cert.justiz.niedersachsen.de heruntergeladen werden.

2. **Anfordern** eines persönlichen S/MIME-E-Mail-Zertifikats von einem der Zertifikatsdiensteanbieter aus der Übersicht im Anhang und Zuweisen zum persönlichen E-Mail-Konto in den entsprechenden Optionen der eingesetzten E-Mail-Software

3. **Senden** einer signierten E-Mail an den Kommunikationspartner in der Nds. Justiz

4. **Erhalt** einer signierten E-Mail von dem Kommunikationspartner in der Nds. Justiz. Die signierte E-Mail enthält das Benutzerzertifikat des Kommunikationspartners.

5. **Anlegen** eines Kontakts für den Kommunikationspartner in der Nds. Justiz im eingesetzten E-Mail-Programm und zuweisen des entsprechenden Benutzerzertifikats zum angelegten Kontakt

6. **Auswählen** der Verschlüsselungsoption S/MIME beim Verfassen einer E-Mail an den Kommunikationspartner in der Nds. Justiz.

## 4. Anleitung PGP

Für die sichere Kommunikation per PGP kann aufgrund der technischen Vielfalt keine allgemeingültige Anleitung zur Verfügung gestellt.

Zur sicheren Kommunikation per PGP ist ein manueller Schlüsselaustausch notwendig.

Dazu nehmen Sie bitte Kontakt mit dem Kommunikationspartner in der Nds. Justiz auf. Dieser wird dann mit Ihnen den Schlüsselaustausch durchführen!